(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 May 2003 (22.05.2003)

PCT

(10) International Publication Number
WO 03/042988 A1

(51) International Patent Classification[7]: G11B 7/007, H04L 9/00, H04N 7/10, 7/16, 7/167, 17/00

(21) International Application Number: PCT/US02/36970

(22) International Filing Date:
15 November 2002 (15.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/335,112 15 November 2001 (15.11.2001) US

(71) Applicants *(for all designated States except US)*: SONY CORPORATION [JP/JP]; ** (JP). SONY MUSIC, INC. [US/US]; ** (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: HUGHES, David [US/US]; New York, NY (US).

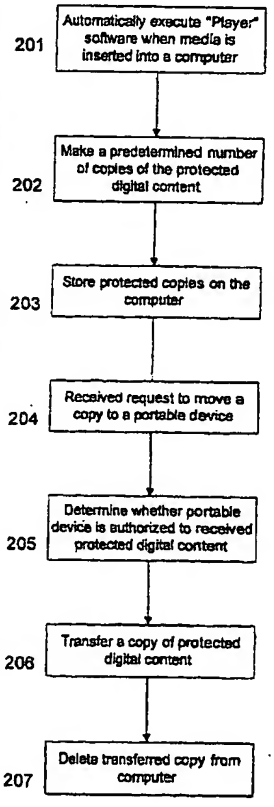
(74) Agents: FLOCK, John, et al.; Kenyon & Kenyon, One Broadway, New York, NY 10004-1050 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR CONTROLLING THE USE AND DUPLICATION OF DIGITAL CONTENT DISTRIBUTED ON REMOVABLE MEDIA



(57) Abstract: Systems and methods for controlling the use and duplication of digital content distributed on removable media are described. In accordance with embodiments of the present invention digital content is protected by allowing a particular number of protected (e.g., encrypted) copies of the digital content to be made (202, 203). Typically, these copies may only be used on and moved between authorized devices (204, 205, 206). In one embodiment, if copies are desired, the maximum number of allowable copies of the protected digital content are made and stored on a computer's hard drive when the storage medium (e.g., a CD) containing the content is inserted into the computer (201, 202, 203). Each copy can then be moved but not copied to other devices (e.g., portable solid state devices) (204, 205, 206). In an alternative embodiment, the storage medium containing the digital content is writable (e.g., a CD-R). When the storage medium is inserted into the computer, the computer writes information to the storage medium which regulates future copying and playing of the digital content on the storage medium (404).

WO 03/042988 A1

European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR CONTROLLING THE USE AND DUPLICATION OF DIGITAL CONTENT DISTRIBUTED ON REMOVABLE MEDIA

This application claims the benefit of U.S. Provisional Application No. 60/335,112, entitled "System And Method For Controlling The Use And Duplication Of Digital Content Distributed On Removable Media", filed November 15, 2001, which is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention is generally directed to controlling the use and copying of digital content which is distributed on removable media.

BACKGROUND

In recent years, the development of digital audio compression technology coupled with the introduction of inexpensive portable audio devices has allowed consumers to carry, literally in their pocket, entire libraries of high quality music to be enjoyed almost anywhere while engaged in almost any activity. These portable devices generally use solid-state memory or miniature computer hard drives to hold hundreds or thousands of megabytes of compressed audio. In order to move music from traditional media (e.g., a Compact Disc™ containing Redbook audio) to the portable device, a consumer generally uses computer software to "rip" the CD and create files containing the compressed audio using an algorithm such as Moving Picture Experts Group (MPEG) Audio Layer 3 (commonly known as MP3). These files may then be copied to the portable device.

An unfortunate side effect of this revolution in audio compression technology has been a substantial increase in copyright infringement and piracy through file swapping over the Internet. Although sharing music with friends and acquaintances via recordable cassette tape and other physical media has been going on for years, high quality audio compression technology combined with one of any number of file swapping software programs can now allow a single consumer to purchase a single copy of an album and almost instantaneously share it with thousands of other individuals worldwide. While some sharing of music among acquaintances can serve to promote a new album or musical act resulting in increased sales, virtually unlimited sharing can drastically erode sales.

A number of potential solutions have been proposed to combat copyright infringement and unlimited copying. Many of these solutions include digital rights management (DRM) schemes which manage virtually every use of the digital content. However, in their present form, these solutions can be difficult and inconvenient to use. Other solutions simply use "anti-ripping" technology to prevent the Redbook audio of a CD from being read by a computer (thus preventing the CD from being ripped) while still allowing it to be read by home stereo equipment. However, this prevents the consumer from making a personal-use copy for use only on the consumer's portable device.

It would be useful to have a solution which prevents or reduces the unlimited file swapping that results in copyright infringement while preserving flexibility and ease of use for the consumer.

SUMMARY

The present invention provides devices, systems and methods for controlling the use of digital content so that, for example, the number of copies made of the content may be controlled or limited without greatly restricting the consumer's ability to use and enjoy the content. This may be accomplished by, for example, storing on a medium a protected copy of the digital content along with a copy of the digital content which is unreadable by a computer system.

In one possible embodiment of the present invention, the removable medium is a CD that contains both standard Redbook audio tracks which have been protected with anti-ripping technology (i.e., the section of the CD with these tracks cannot be read by a computer CD drive or computer DVD drive, but can be read by, for example a stereo system) as well as a computer readable section of the CD. The computer readable section of the CD contains protected versions of the same audio tracks in a compressed format. Software for playing, using or making copies of these compressed tracks may also be provided on the CD. The CD may be used like a conventional CD in stereo equipment or may be used in a computer to provide the consumer with a limited number of copies of the digital content for use in a portable device or on other computers.

When the removable media is placed in the consumer's computer system, the software may allow the consumer to play or otherwise use the content directly as well as allowing the consumer to make a limited number of copies which may be transferred to a portable device or transferred to another computer. The number of copies that can be

made may be limited by one or more of a number of factors including, for example, the number of copies currently on the computer, the number of copies ever made, or whether copies were previously made on another computer. These copies are all stored on the computer when they are made and may then be transferred to the portable device or to another computer, or they may simply be played by the software without the removable medium needing to be in the computer.

In another possible embodiment of the present invention, the removable media is a writable CD, for example a CD-R or CD-RW that contains protected Redbook audio, a protected, compressed version of the same audio, and software for accessing the compressed audio. The CD may be used like a conventional CD in stereo equipment or may be used in a computer to provide the consumer with a limited number of copies of the digital content for use in a portable device or on other computers. The software may then write information onto the CD about the copies made or the circumstances under which the copies were made.

These embodiments and variations to them, as well as other possible embodiments, are described in more detail below.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 illustrates an overview of an example of one embodiment of the present invention.

Figure 2 illustrates a flowchart of one aspect of an embodiment of the present invention.

Figure 3 illustrates a flowchart of one aspect of an embodiment of the present invention.

Figure 4 illustrates a flowchart of one aspect of an embodiment of the present invention.

DETAILED DESCRIPTION

In accordance with example embodiments of the present invention, a medium, especially a removable storage medium, such as a CD, stores digital music files on it that have been encrypted or protected from unauthorized access in some other fashion. The digital files may contain, for example, audio music that has been compressed using a well-known audio compression algorithm such as Sony's ATRAC™, MP3, Microsoft

Windows' Media Audio™ (WMA), but the audio may be at "normal" CD fidelity. The CD may also contain software for decrypting and playing the digital files. In addition, the CD may contain standard Redbook audio that has been protected using, for example, Macrovision, Inc.'s SafeAudio™ or some other "anti-ripping" technology to prevent copying the CD using a computer. This allows typical home or car stereo equipment to play the Redbook audio directly from the CD with little to no loss of fidelity without compromising the security and control features of the present invention. The removable storage medium is not limited to CDs, but may also include MiniDisc™, Digital Versatile Disc (DVD), and other forms of removable storage media. The digital content is not limited to music but may also include other content, such as audio, video, or multimedia.

For example, as shown in Fig. 1, an embodiment of the present invention may include a storage medium 101 containing protected Redbook audio, which is unreadable on a computer, as well as computer readable, encrypted digital audio files (and possibly the "player" software required to use the encrypted audio files). The storage medium 101 may be used in a computer 102 which may communicate with a portable device 103. The computer 102 may already have the player software on it or it may be installed from the storage medium. The player software may be used to transfer copies of the encrypted digital audio files to the portable device 103 as further described below.

In one example embodiment of the present invention, control over the copying of digital content on a removable storage medium is achieved by making a limited number of protected copies of the digital content, storing the copies on a computer, and allowing the copies to be moved to other devices with no further copies being made. In this embodiment (as briefly illustrated in Figs. 1 and 2), when the storage medium is inserted into or connected to a computer, the player software on the CD is automatically executed (Step 201). The player software installs itself on the computer and then may make a predetermined number of copies (e.g., 4 copies) of the digital files on the CD (Step 202) and stores them on the computer (e.g., on the hard drive) (Step 203). Each copy of the digital files is encrypted and may be decrypted and played only by the player software or other authorized software. The player software may also be used to move (not copy) the digital files to other devices. All copying and moving of the digital files may be performed using a secure authenticated channel (SAC). For example, as illustrated in Fig. 2, a user may connect a portable device to the computer and request that a digital file be transferred to the device (Step 204). The player software may contact the portable device

and verify that the device is authorized to receive the digital content (Step 205). For example, the player software may verify that the device has certain content protection and/or tamper resistance capabilities so that the content will not be vulnerable to unauthorized access while stored in the device. The player software can also perform an identity authentication routine to insure that the portable device is not an "imposter" using, for example, a unique authentication ID number or similar means. Once the device has been authenticated, the player software transmits one of the copies of the requested digital file and the information necessary to use it (e.g., its decryption key) to the portable device (Step 206). After or contemporaneously with transmission of the copy of the digital file, the player software deletes that copy from the hard drive of the computer (Step 107); thus, the digital file is "moved" to the portable device and no additional copies have been created.

The movement of the copies to other devices may also be controlled. For example, the player software may be configured such that copies of digital files can only be moved to authenticated portable devices. Alternatively, the player software may be configured to allow copies to be moved to any authenticated device including other computers that are equipped with authenticated player software, thus allowing some limited file swapping. The player software may also be configured to allow copies to be moved only once using, for example, controls similar to those of Serial Copy Management Systems (SCMS) (e.g., when the copy is moved to another device, the copy is marked in some fashion so that the device to which it is moved will not allow it to be moved again).

Additionally or alternatively, copies of files made by the player software may also include additional information that may be used to track unauthorized copies or copies that have had their encryption or protection broken. For example, each copy may include information that uniquely identifies the computer on which the copy was originally made. Alternatively, a unique identification number may be encoded on the storage medium and then transferred to each of the copies of the digital files. Thus, each copy would contain information that would uniquely identify the particular storage medium from which it was originally made. This identification information may be stored in various ways within the copies. For example, the decryption key for each file may be based on the identification information such that the identification information could be later extracted from the key, if desired.

The number of copies of the digital files that are made when the storage medium is placed in the computer may be determined in several ways. For example, the player software may be configured to make a particular number of copies (e.g., 4 copies) of every digital file on a CD, every time the CD is inserted into a computer. Alternatively, the player software may be configured to set a maximum or default number of copies that may be made and the user may be able to elect to have a smaller number of copies made due to a limited amount of available storage space on the computer, for example. The number of copies to be made may also vary based on the storage medium. For example, each CD may be encoded with information that specifies how many copies the player software may make.

In this example embodiment, as illustrated in Fig. 3, when the storage medium is inserted into the computer (Step 301), the player software may also determine if copies of the digital files already exist on the computer from, for example, a previous use of the storage medium in the computer (Step 302). If copies do not exist the player software will make the predetermined number of copies (Step 303). If copies already exist, the player software will not make additional copies (Step 304). Alternatively, the player software may be configured to use the same filenames and place copies in the same location every time copies are made. Thus, the player software need not check for existing copies, but if any did exist they would simply be overwritten by the new copies.

The player software may also be configured so that it can play the digital files directly from the storage medium without making any copies. Thus, if a user does not wish to make any copies or if the maximum number of copies have already been made from the storage medium, the storage medium may still be used to play the audio, so long as the storage medium is in the computer at the time.

In an alternate embodiment, control over the copying of digital content on a removable storage medium is achieved by writing information to the storage medium upon the first use of the storage medium and using that information to determine future usage (e.g., copying, moving, playing, viewing) of the digital content. In this embodiment the removable storage media may include, for example, a writable medium such as CD-R or MiniDisc. In this embodiment as illustrated in Fig. 4, for example, when a CD is placed into a computer, the player software on the CD is automatically executed and installs itself on the computer (Step 401). The player software may then make copies of the digital files on the CD and store them in the computer (e.g., on the hard drive) (Steps 402 and 403.

Contemporaneously with the copies being made, the player software writes information to the CD (Step 404). The next time the player software is run (e.g., the next time the storage medium is placed into a computer), the player software can read the information from the CD and use it to determine if more copies of the digital files can be made. Any copies of the digital files made under this embodiment may be moved but not copied, similar to the previously described embodiment.

The information written to the storage medium may include information that uniquely identifies the computer on which the copies were made such as an identification number (e.g., the serial number of the operating system) or a hardware description of the computer (e.g., a list of the hardware components in the computer such that it is unlikely that two computers would be identical). Thus, for example, the storage medium may be "bound" to the computer. Alternatively, the information may include how many copies have been made of the digital files, or how many additional copies may be made of the digital files. For example, the player software may not allow copies of the digital files to be made on any computer other than the one on which copies were made initially, or the player software may not allow more than 4 total copies to be made regardless of on which computer they are made. Another alternative is that once the maximum number of copies have been made, the player software may erase the digital files or the decryption keys from the storage medium.

The player software used by embodiments of the present invention may be universal software that could be used with any storage medium that used the protection system of the invention. For example, each protected CD may have a copy of the same player software on it and that player software reads the digital files and their respective decryption information off of the CD for installation on the computer. If the universal player software already exists, it is not necessary to copy the software again and merely the digital files and any information necessary to use them is copied. File copies and decryption information for multiple CDs may then be maintained by a single copy of the player software using, for example, a secure database. Alternatively, it may be desirable to have multiple versions of the player software, for example, one specific to each music distributor. Under this alternative, each music distributor may be responsible for its own software, reducing the amount of coordination necessary to successfully implement embodiments of the present invention. The software would work similarly to the universal player, but each specific version would only work with CDs produced by a particular

company. The present invention may also be implemented with player software versions that are unique to each particular album and are maintained separately from the software for all other albums. These unique versions may have special features such as enhanced or increased security levels. Optionally, the player software may also be downloaded over a network such as the Internet.

In accordance with example embodiments of the invention, the integrity of the player software is maintained in order to ensure the security and control provided by the invention. If the player software is tampered with, it may be possible to gain access to the digital content in an unprotected form. When the player software is executed directly from the storage medium, it is unlikely to have been tampered with. However, once installed on the computer, it becomes vulnerable to reverse engineering and other tampering. One possible method of authenticating the integrity of the player software is to have the player software or some portion of the player software be reinstalled on the computer each time the storage medium is inserted into the computer. Any existing player software that may have been tampered with is simply overwritten, erased, or disabled. Another method of protecting the player software is to have part of the player software, or another software program on the storage medium that executes when the medium is inserted, check the player software previously installed on the computer using a digital signature, a checksum, or any other well known method of integrity checking. If the player software fails the integrity check, it is rejected or overwritten. Alternatively, the integrity checking software may connect to a central server using a network and request that server to perform an integrity checking routine on the player software and even the storage medium itself.

In the example embodiments of the present invention, the copies of the digital files may be encrypted or protected in a variety of ways. One possible method of protecting the files is to encrypt each copy of each file with a unique key. For example, the player software loads each encrypted song or track from a CD, decrypts it using the appropriate key, makes 4 copies of the track, and then encrypts each copy with a different key. This method would provide the greatest level of security against unauthorized access, but would also require more time to perform the copying operation and would require managing a much greater number of keys. Alternatively, all the copies of a particular track made on a particular computer could be encrypted with the same key or all copies of a track could be encrypted with the same key regardless of what computer on which they were made. The encryption keys may be generated locally on the computer performing

the copying, downloaded from a central server, or already present on the storage medium. The encryption algorithm used could be, for example, any symmetric or asymmetric encryption algorithm that provides a balance of adequate protection without being so computationally intensive that it adversely effects the performance of the computer or portable device.

The present invention is not limited to the specific embodiments described. It is expected that those skilled in the art will be able to devise other implementations that embody the principles of the present invention and remain within its scope.

WHAT IS CLAIMED IS:

1. A digital storage medium having stored thereon digital data comprising:

a plurality of segments of digital content data stored on the storage medium and adapted to be unreadable on a computer system; and

a protected version of the plurality of segments of digital content data stored on the storage medium.

2. The digital storage medium of claim 1 wherein the plurality of segments of digital content data are Redbook audio tracks.

3. The digital storage medium of claim 2 wherein the Redbook audio tracks are adapted to be readable only on stereo equipment.

4. The digital storage medium of claim 2 wherein the protected version of the plurality of segments of digital content data are encrypted, compressed copies of the Redbook audio tracks.

5. The digital storage medium of claim 4, further comprising:

a plurality of instructions stored on the storage medium and adapted to be executed by the computer system, the instructions which, when executed, define a series of steps to be used to control the use of the protected version of the plurality of segments of digital content data, said steps comprising:

producing a limited number of copies of the protected version of the plurality of segments of digital content data;

storing said limited number of copies on a storage device connected to the computer system; and

controlling access to said limited number of copies.

6. The digital storage medium of claim 5 wherein said access is controlled by preventing copying of said limited number of copies.

7. The digital storage medium of claim 5 wherein said access is controlled by only allowing said limited number of copies to be transferred to an authenticated device.

8. The digital storage medium of claim 6 wherein a transferred copy is marked to indicate that it may not be further transferred.

9. The digital storage medium of claim 7 wherein said authenticated device is another computer system.

10. The digital storage medium of claim 7 wherein said authenticated device is a portable audio device.

11. The digital storage medium of claim 5, said steps further comprising:

writing information to said digital storage medium regarding the production of the limited number of copies.

12. The digital storage medium of claim 11, said steps further comprising:

determining the limited number of copies to be produced based on information previously written to the digital storage medium.

13. The digital storage medium of claim 12 wherein said information written to the digital storage medium includes information identifying the computer system.

14. The digital storage medium of claim 13 wherein said information identifying the computer system includes information about the computer system's hardware configuration.

15. The digital storage medium of claim 12 wherein said information written to the digital storage medium includes information identifying the number of copies made.

16. A method for controlling the use of protected digital content distributed on removable media, comprising:

reading the removable media with a computer system;

producing a predetermined number of protected copies of the digital content;

storing said protected copies on a storage device connected to the computer; and

moving at least one of said protected copies to another device.

17. The method of claim 16 wherein the number of protected copies is determined based on information stored on the removable media.

18. The method of claim 17 wherein the information stored on the removable media includes information identifying a computer system on which copies were previously made.

19. The method of claim 18 wherein said identifying information includes information about the hardware components in the computer system.

20. The method of claim 17 wherein the information stored on the removable media includes information about how many copies have been previously made.

21. The method of claim 16 wherein moving at least one of said protected copies to another device comprises:

copying said at least one of said protected copies to another device; and

deleting said at least one of said protected copies from the computer system.

22. The method of claim 16, further comprising:

authenticating said another device before moving said at least one of said protected copies.

23. The method of claim 22 wherein authenticating said another device includes determining whether said another device is authorized to receive protected copies of the digital content.

24. The method of claim 23 wherein said another device is another computer system.

25. The method of claim 23 wherein said another device is a portable device.

26. The method of claim 16, further comprising:

executing software stored on the removable media to perform the steps of producing and storing said predetermined number of protected copies.

27. The method of claim 26, further comprising authenticating the integrity of the software stored on the removable media.

28. The method of claim 27, further comprising:

installing, on the computer system, the software stored on the removable media.

29. A method for controlling the use of protected digital content distributed on removable media, comprising:

reading the removable medium with a computer system;

producing a limited number of protected copies of the digital content;

storing said limited number of protected copies on a storage device connected to the computer system;

controlling access to said limited number of protected copies based on control information stored on the removable medium.

30. The method of claim 29 wherein the control information includes information identifying a computer system on which copies were previously made.

31. The method of claim 30 wherein said identifying information includes information about the hardware components in the computer system.

32. The method of claim 29 wherein the control information includes information about how many copies have been previously made.

33. The method of claim 29 further comprising:

transferring at least one of said protected copies to an authenticated device.

34. The method of claim 29 further comprising:

including identification information in each of said protected copies identifying the particular removable media from which it was copied.

35. The method of claim 34 further comprising:

including identification information in each of said protected copies identifying the computer system on which it was made.

36. The method of claim 29 further comprising:

including identification information in each of said protected copies identifying the computer system on which it was made.

37. A digital storage medium having stored thereon digital data comprising:

a plurality of segments of digital content data adapted to be unreadable on a computer system;

a protected version of the plurality of segments of digital content data; and

executable software for controlling access to said protected version of the plurality of segments of digital content data,

wherein said software produces a limited number of copies of said protected version of the plurality of segments of digital content data and allows these copies to be transferred to authenticated devices so long as no additional copies are produced.

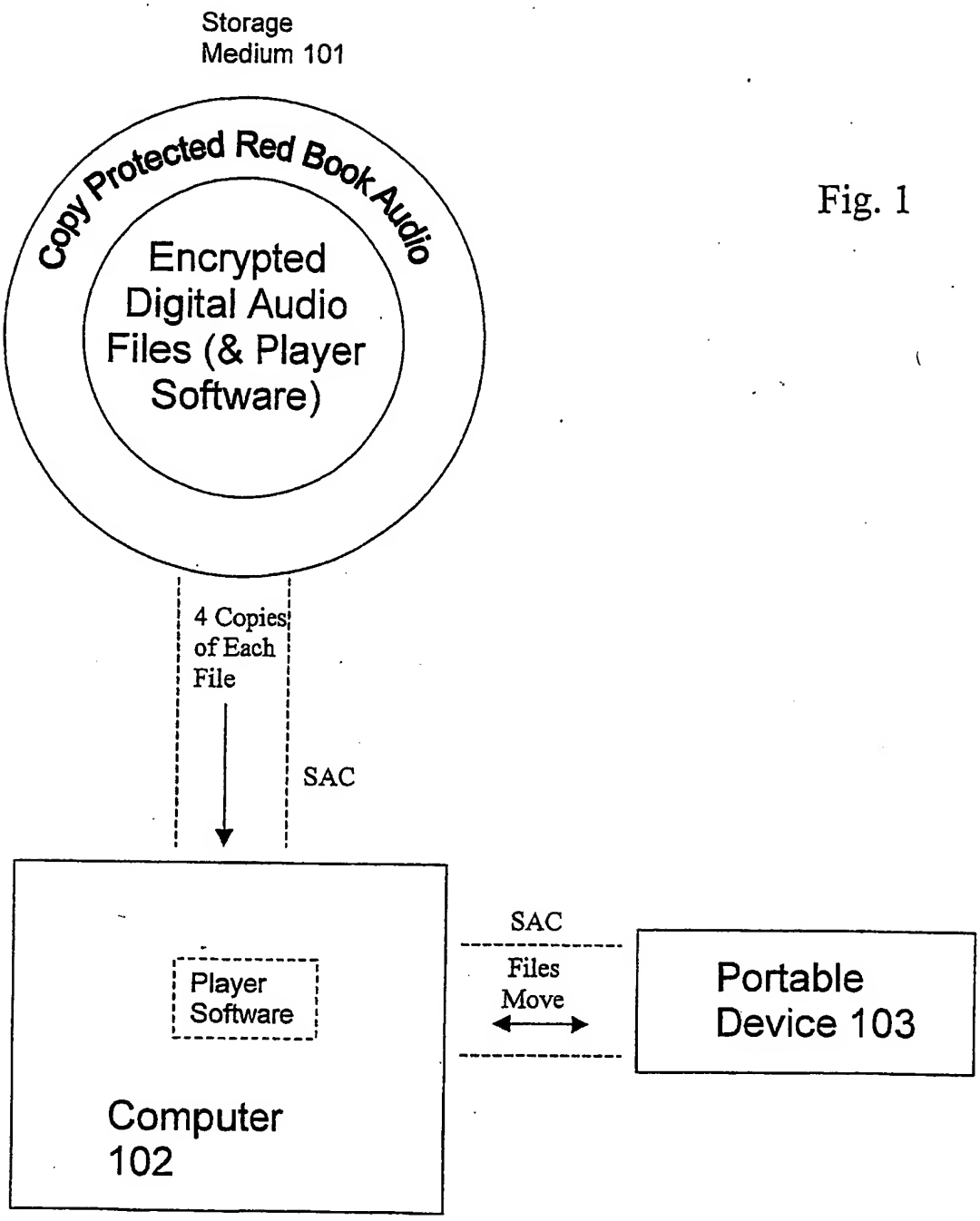

Storage Medium 101
Copy Protected Red Book Audio
Encrypted Digital Audio Files (& Player Software)
4 Copies of Each File
SAC
Player Software
Computer 102
SAC
Files Move
Portable Device 103

Fig. 1

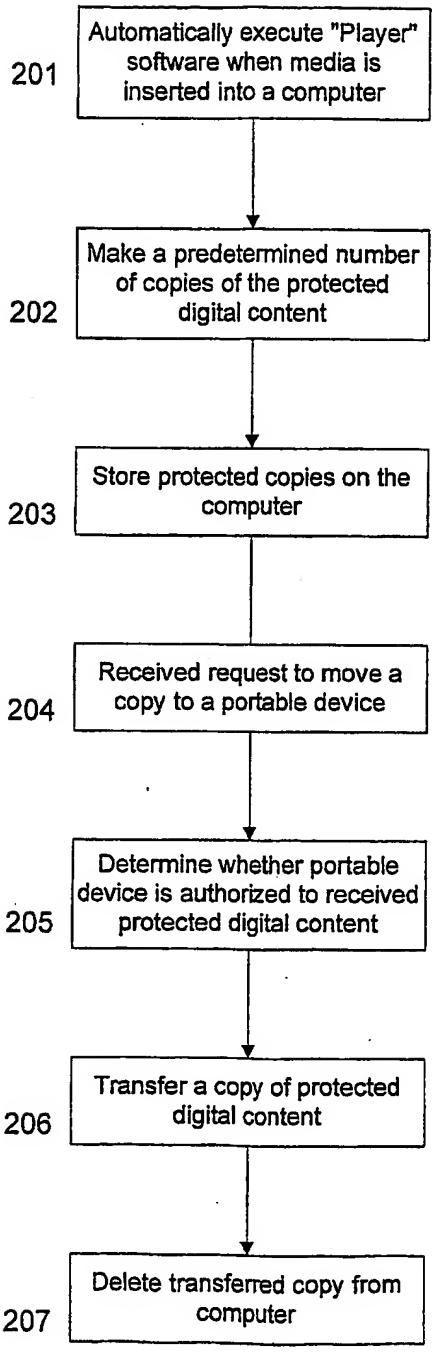

201
Automatically execute "Player" software when media is inserted into a computer
202
Make a predetermined number of copies of the protected digital content
203
Store protected copies on the computer
204
Received request to move a copy to a portable device
205
Determine whether portable device is authorized to received protected digital content
206
Transfer a copy of protected digital content
207
Delete transferred copy from computer

Fig. 2

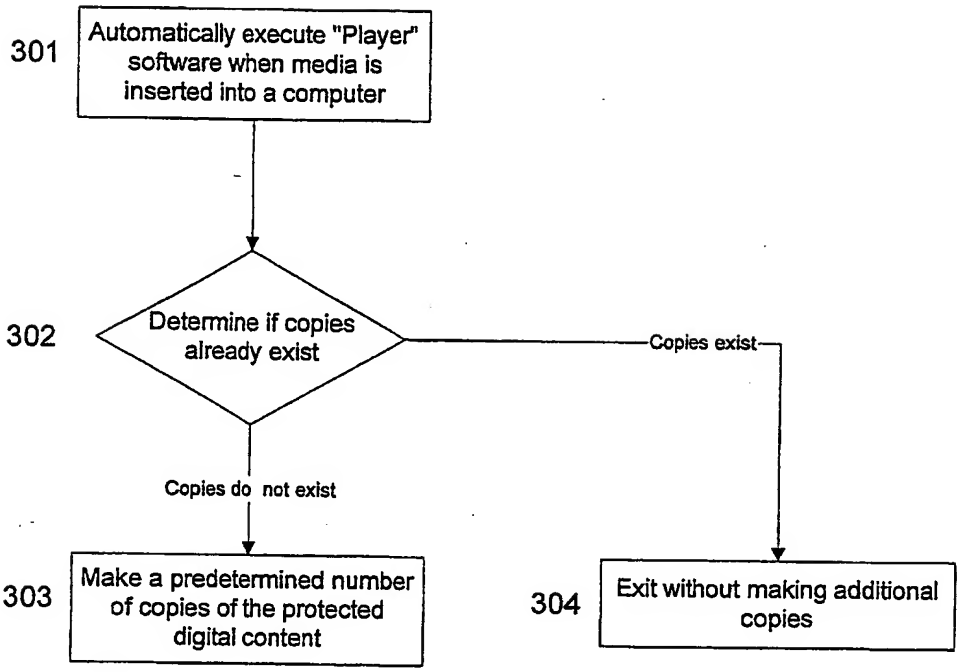

301
Automatically execute "Player" software when media is inserted into a computer
302
Determine if copies already exist
Copies exist
Copies do not exist
303
Make a predetermined number of copies of the protected digital content
304
Exit without making additional copies

Fig. 3

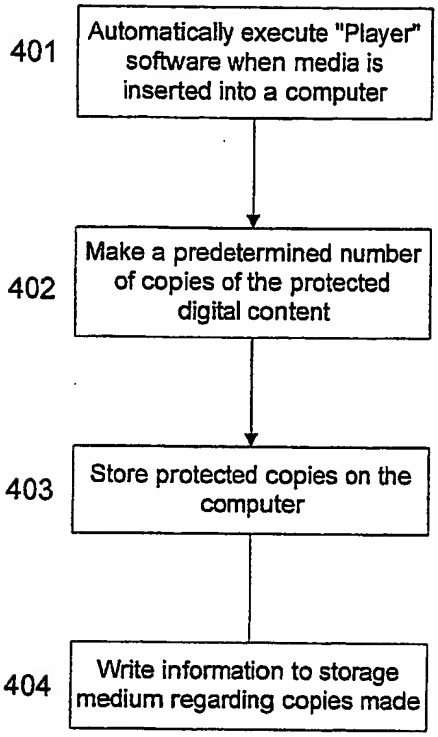

401
Automatically execute "Player" software when media is inserted into a computer
402
Make a predetermined number of copies of the protected digital content
403
Store protected copies on the computer
404
Write information to storage medium regarding copies made

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/36970

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G11B 7/007; H04L 9/00; H04N 7/10, 7/16, 7/167, 17/00

US CL :Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/161, 168, 176, 181, 200, ; 380/4, 5, 9, 23, 25, 28, 30, 49, 277, 278, 281, 283; 705/1, 14, 161, 168, 170, 178, 193, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST

search terms: copying, protection, authorized, copies

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,963,909 A (WARREN et al) 05 October 1999, Abstract, col. 1 line 35 to col. 2, line 25, col. 5, line 60 to col. 6, line 57, col. 10, lins 2-3, col. 11, line 2.	1-36
Y	US 6,108,420 A (LAROSE et al) 22 August 2000, Abstract, col. 17, lines 10-12.	1-36
Y	US 5,896,255 A (MARDIROSSIAN) 20 April 1999, Figure 1, col 4 to col. 5, col. 6 to col. 7.	1-36
Y	US 6,154,206 A (LUDTKE) 28 November 2000, col. 10, lines 49-55.	1-36
Y	US 6,141,753 A (ZHAO et al) 31 October 2000, col. 5 to col. 6	1-36

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 23 FEBRUARY 2003	Date of mailing of the international search report 26 MAR 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LY V. HUA Telephone No. (703) 305-9684

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/36970

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/36970

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,757,534 A (MATYAS et al) col. 1 to col. 2.	37
Y	US 5,845,065 A (CONTE et al) 01 December 1998, col. 1.	37

Form PCT/ISA/210 (continuation of second sheet) (July 1998)*